2024 NIST PSCR UAS WORKSHOP:

CYBERSECURITY AND ARTIFICIAL INTELLIGENCE RISK MANAGEMENT FOR UNCREWED AIRCRAFT SYSTEMS (UAS) IN PUBLIC SAFETY

February 7-8, 2024

In this packet:

- Agenda
- Speaker bios
- QR codes for participation
- Public safety scenarios
- Example Top 10 questions
- Glossary of terms
- PSCR contact information

NIST PUBLIC SAFETY COMMUNICATIONS RESEARCH

UNCREWED AIRCRAFT SYSTEMS

UNCREWED AIRCRAFT SYSTEMS (UAS)

February 7-8, 2024 Workshop

Agenda

Day 1 – February 7, 2024

9:00 – 9:30 **Event Introduction**

Ellen Ryan – *NIST Public Safety Communications Research*
Terese Manley – *NIST Public Safety Communications Research*
Raymond Sheh – *NIST Public Safety Communications Research*

9:30 – 10:30 **Presentations – Public Safety Responder Risk Management**

Katie Thielmeyer – *DroneResponders*
Barry Brennan – *Flying Lion*
Bart Ramaekers – *CARMA Police*
Jason Day – *Texas Department of Public Safety*

10:30 – 10:45 **Break**

10:45 – 11:00 **Q&A**

11:00 – 11:45 **Presentations – Government and Regulatory Agency Risk Management**

Billy Bob Brown – *DHS Cybersecurity & Infrastructure Security Agency*
Mike O'Shea – *Federal Aviation Administration*
Preet Bassi – *Center for Public Safety Excellence*

11:45 – 12:45 **Presentations – AI / Cybersecurity**

Jesse Dunietz – *NIST Information Technology Laboratory*
Apostol Vassilev – *NIST Information Technology Laboratory*
John Beltz – *NIST Public Safety Communications Research*
Don Harriss – *NIST Public Safety Communications Research*

12:45 – 1:45 **Lunch**

**Note: exact times subject to change*

Day 1 – February 7, 2024 (cont'd)

1:45 – 2:00 **Q&A**

2:00 – 3:15 **Presentations – Connected Systems and Society**

Jay Stanley – *American Civil Liberties Union*
Dorothy Spears-Dean – *Virginia Department of Emergency Management*
Ryan Bracken – *DroneSense*
Michelle Hanlon – *Center for Air and Space Law, University of Mississippi*
Stephen Luxion – *Alliance for System Safety of UAS through Research Excellence*

3:15 – 4:45 **Interactive UAS Operation Scenario – Assessing Risk Management Gaps**

4:45 – 5:15 **Day 1 Recap**

Day 2 – February 7, 2024

9:00 – 9:30 **Day 1 Recap and Day 2 Introduction**

9:30 – 10:15 **Q&A**

10:15 – 10:45 **Presentation – Experiences with Self-Driving Cars**

Missy Cummings – *George Mason University*

10:45 – 11:00 **Break**

11:00 – 12:30 **Interactive UAS Operation Scenario – Identifying Solutions to Gaps**

12:30 – 2:00 **Lunch**

2:00 – 3:00 **Deliverable Workshop and Prioritization Exercise**

3:00 – 3:30 **Event Recap and Next Steps**

***Note: exact times subject to change*

UNCREWED AIRCRAFT SYSTEMS (UAS)

February 7-8, 2024 Workshop

Speaker Bios

Day 1 – February 7, 2024

9:00 – 9:30 **Event Introduction**

Ellen Ryan – *NIST Public Safety Communications Research*

Ellen Ryan is the Deputy Division Chief for the Public Safety Communications Research (PSCR) Division, within the Communication Technology Laboratory (CTL), NIST. She develops and manages best-practices and processes for the PSCR Division in operational areas such as lab deployment, safety, and security. In addition, she leads the PSCR Open Innovation (OI) team and ensures all aspects of the OI programs are planned and executed according to the OI standard operating procedures (SOP) and meet the goals of the PSCR mission. Ms. Ryan's background is in operations, systems verification and new product development, with over 20 years of industry experience in telecommunications research and development. Her technical areas of expertise include telecommunications networks. Ms. Ryan's education includes a Master's of Science degree in Computer Science and two Bachelor's of Science degrees, one each in Computer Science and Geography.

Terese Manley – *NIST Public Safety Communications Research*

Terese Manley is the UAS Portfolio Lead and UAS Prize Manager at NIST PSCR. In this role, she manages internal and external research to enhance public safety UAS programs as it relates to emerging technologies. She engages external researchers and working groups including federal agencies, state/local first responders, industry experts, and academia with the goal of advancing UAS technology and U.S. economic development. Prior to PSCR, Ms. Manley was an industry lead for the Interdisciplinary Telecom Graduate Program at CU Boulder and, for most of her career, held management and engineering positions at Sprint Nextel Corporation.

Raymond Sheh – *NIST Public Safety Communications Research*

Dr. Raymond Sheh is the Uncrewed Aircraft System (UAS) Research Lead for the UAS Portfolio, and a Guest Researcher, at the Public Safety Communications Research Division (PSCR) of the U.S. National Institute of Standards and Technology (NIST). He is also an Adjunct Associate Research Scientist at Johns Hopkins University. He previously held appointments as a Guest Researcher at the Intelligent Systems Division of NIST, and as a Research Professor at Georgetown University, where he worked closely with researchers, manufacturers, vendors, public safety end users, and international partners to develop measurement science approaches to evaluating the performance of ground, aerial, and underwater robotic systems used in applications such as search and rescue, hazardous materials cleanup, and incident response. He was also a Senior Lecturer at Curtin University in Western Australia, where he developed and taught undergraduate and graduate units in artificial intelligence (AI), cyber security, and computer science. His current work at PSCR revolves around trusted autonomous systems in public safety applications, with a focus on UAS. This includes the areas of performance measurement, explainable AI, cybersecurity, reliable communications, and risk management for robotic and cyberphysical systems. He also works on developing and running academic research competitions for the next generation of intelligent robots in public safety applications that push the state-of-the-science in capabilities while also educating competitors about the need to manage and address cybersecurity and AI risks. Ask him about his experience with robotic lion cubs and his superhero alter-ego's efforts to avert the next AI winter.

9:30 – 10:30 **Presentations – Public Safety Responder Risk Management**

Katie Thielmeyer – *DroneResponders*

Katie Thielmeyer is a firefighter/paramedic and FAA Part 107-certified remote pilot who assists public safety agencies implement best-of-class drone programs based on ASTM and National Institute of Standards and Technology (NIST) small unmanned aircraft systems (sUAS) flight standards. She is regarded as a subject matter expert in the use of sUAS for mission-critical public safety applications. Ms. Thielmeyer serves as the Risk Reduction Officer with the Woodlawn (Ohio) Fire Department, where she oversees the Risk Reduction Division, delivering an array of essential services including fire & EMS response, community outreach, and fire prevention programs. In 2018, Thielmeyer created the Emergency Services Special Operations (ESSO) sector within the Risk Reduction Division to implement a public safety unmanned aviation program focused on sUAS response. That team, UAS 500, in collaboration with other fire and law agencies, now provides mutual assistance for regional deployments in the Cincinnati area and beyond. Katie also serves as a project manager and principal investigator with DRONERESPONDERS, the world's fastest-growing non-profit program supporting the use of sUAS by public safety agencies and emergency services around the globe. In this capacity, Ms. Thielmeyer oversees DRONERSPONDERS' partnership with NIST, as well as other specialized initiatives.

Day 1 – February 7, 2024 (cont'd)

9:30 – 10:30 **Presentations – Public Safety Responder Risk Management (cont'd)**

Barry Brennan – *Flying Lion*

Barry Brennan is the President and founder of Flying Lion, Inc. (FLI), a full service sUAS Solutions Company. As President, Barry manages all aspects that contribute to FLI's continuous pursuit of excellence. Mr. Brennan has developed several drone air support programs for Public Safety Agencies, Corporations, and Municipalities. Additionally, he has designed and developed an Association for Unmanned Vehicles Systems International (AUVSI) XCELLENCE Award winning sUAS Curriculum and Flight Training for Community Colleges throughout Southern California. In the past, for his operational expertise he has been a five-time Toyota Kaizen Award recipient and recent two-time Toyota vendor of the year award winner. Beyond Mr. Brennan's business success, he is proud of his strong philanthropic background. These efforts have resulted in two personally humbling awards: Big Brother of the Year and Reserve Police Officer of the Year. Mr. Brennan began his career on a path that is rare among other business executives. Having earned his Bachelor's degree in Political Science from the University of California, Berkeley, Mr. Brennan's goal was to use the multiple disciplines of his degree - history, politics, economics, and social studies, to compliment his natural extroverted personality to develop his skills as professional business administrator. Mr. Brennan later in his career acquired his Master's in Business Administration from the University of Southern California.

Bart Ramaekers – *CARMA Police*

Bart Ramaekers is the Chief Inspector of Police at CARMA Police Zone and Senior Lecturer for the UAS State Operator PLOT Limburg in Belgium. Police CARMA is a dynamic and extremely diverse police zone that forms an essential part of the integrated police. With a team of more than 400 colleagues, they are committed to the safety of ~177,274 residents in two cities and six municipalities. At CARMA Police, the emphasis is on community-oriented policing, in which they fulfill seven crucial functions: community work, reception, intervention, victim assistance, local investigation, maintenance of public order and traffic management. Implementing their Zonal Safety Plan is an essential part of their efforts. The name 'CARMA' has both a geographical and symbolic meaning, referring to Carboniferous, Meuse and karma.

Jason Day – *Texas Department of Public Safety*

Jason Day is the Director of Unmanned Aircraft at the Texas Department of Public Safety, bringing with him a wealth of experience from his 27-year tenure military, civilian, & public safety aviation. Widely recognized as a subject matter expert in the UAS community, Mr. Day specializes in public safety UAS operations & administration. In his role as Director, Mr. Day oversees one of the largest public safety UAS program in the nation with over 300 remote pilots & unmanned aircraft. His primary responsibilities include ensuring compliance with FAA regulations & maintaining the highest standards of safety in the department's UAS program. Texas DPS stands out as one of the most active UAS programs in the United States conducting 50,000 flights in 2023 & a remarkable 12,000 flight hours. Operating within the Aircraft Operations Division of Texas DPS, Mr. Day has actively participated in high-profile UAS missions, including disaster response, tactical operations, overwatch missions, & border operations. Recognized for his expertise in joint manned/unmanned aircraft operations, Mr. Day holds a crucial seat in the Texas Air Operations Center, coordinating UAS operations during declared disasters in the state. As a key member of the Texas HB2340 Committee, Mr. Day played a pivotal role in developing policies, procedures, & training standards for UAS use by public safety agencies during disasters. Mr. Day developed & implemented the UAS Remote Pilot in Command training program for the department, earning recognition in Air Beat Magazine & serving as a template for various federal, state, & local public safety agencies. He has assisted countless public safety agencies across the world in establishing their UAS programs, emphasizing safety, compliance & transparency. Mr. Day's contributions extend to numerous publications on topics related to public safety UAS operations. Actively engaged in the UAS community, Mr. Day is a member of numerous UAS & cUAS working groups & servers on multiple boards.

11:00 – 11:45 **Presentations – Government and Regulatory Agency Risk Management**

Billy Bob Brown – *DHS Cybersecurity & Infrastructure Security Agency*

Billy Bob Brown, Jr., serves as the Executive Assistant Director for Emergency Communications within the Cybersecurity and Infrastructure Security Agency (CISA) since Oct 12, 2020. In this capacity, AD Brown is one of three CISA designated Executive Sponsors, as identified in the Cybersecurity and Infrastructure Security Act of 2018. Brown most recently served as the Associate Director, Priority Telecom Services Sub-Division as well as the Program Manager for both the DHS Level 2 Program Next Generation Networks Priority Services Program and the Level 3 Program Priority Telecommunications Services Program. In this role, he was responsible for providing priority telecommunications services over commercial networks to enable national security and emergency preparedness (NS/EP) personnel to communicate during congestion scenarios across the nation. Previous to this assignment, he served as the Chief Administrative Officer, Office of Emergency Communications (OEC) and worked with a team to develop, coordinate, and implement a Resources Management across the five-year Future Years Homeland Security Program. Prior to this, Brown served as Chief, Regional Coordination Branch, OEC, leading a geographically dispersed team that facilitated operational communications coordination at all levels of government. He advocated key emergency communications initiatives, programs, and activities designed to unify and lead the nationwide effort to improve NS/EP communications capabilities. Prior to joining the OEC in 2008, Brown served as an Operations Analyst with General Dynamics Information Technology and served as a career military officer in the United State Marine Corps as an Infantry Officer. Brown graduated from the United States Air Force Academy with a Bachelor of Science degree and holds a Master of Business Administration from Webster University. He is a certified Project Management Professional (PMP).

Day 1 – February 7, 2024 (cont'd)

11:00 – 11:45 **Presentations – Government and Regulatory Agency Risk Management (cont'd)**

Mike O'Shea – *Federal Aviation Administration*

Michael O'Shea is a Program Manager for the FAA's UAS Integration Office's, Safety & Integration Division where he serves as liaison, facilitator and resource for both public and civil unmanned aircraft integration efforts. Before joining the UAS Integration Office, Mr. O'Shea was a program manager for 17 years in the U.S. Department of Justice's (DOJ) Office of Science and Technology, where he managed the law enforcement aviation technologies program among other duties. As part of his duties at DOJ Mr. O'Shea sat on the Small UAS (Part 107) and Remote Tracking/ID Aviation Rule Making Committees and was the co-author of the MOU between the FAA and DOJ that initiated public safety COAs for UAS. Prior to working at DOJ, Mr. O'Shea spent almost 15 years as a uniformed law enforcement officer. Mr. O'Shea is a graduate of Baker University (Kansas) with a degree in Business and Marketing. Mr. O'Shea holds a FAA Light-Sport Pilot Certificate (Fixed Wing, Gyroplanes and Powered Parachutes) and a Part 107 Remote Pilot Certificate.

Preet Bassi – *Center for Public Safety Excellence*

Preet Bassi is the CEO of the Center for Public Safety Excellence. She previously worked for the International Accreditation Service and has experience at local and state government levels, having worked for the City of Anaheim and the California State Assembly. She has a MPA from the University of Southern California and BAs in Economics and Political Science from UC Davis. She is a Certified Association Executive and holds graduate certificates in Social Innovation Design and Diversity and Inclusion.

11:45 – 12:45 **Presentations – AI / Cybersecurity**

Jesse Dunietz – *NIST Information Technology Laboratory*

Dr. Jesse Dunietz is a computer scientist in the Information Technology Laboratory (ITL) at the U.S. National Institute of Standards and Technology (NIST), where he leads international engagements on AI for NIST's Trustworthy and Responsible AI program. He holds a bachelor's from MIT and a Ph.D. from Carnegie Mellon University (CMU), both in computer science. His technical background includes research in natural language processing at CMU, MIT, Google, and a small startup. He has also trained hundreds of researchers in science communication and written many articles and video scripts for mass media outlets. Prior to his current position, he was a AAAS Science and Technology Policy Fellow at the U.S. Department of State, where he led the Department's international work on AI and human rights.

Apostol Vassilev – *NIST Information Technology Laboratory*

Apostol Vassilev is a research supervisor in the Computer Security Division at NIST. His group's research agenda covers a range of topics in Trustworthy and Responsible AI and Cybersecurity, with a focus on Adversarial Machine Learning (AML), Robust AI for Autonomous Vehicles, AI bias, meta learning with large language models (LLMs), Multi-Party Threshold Cryptography, novel approaches to cybersecurity testing and measurement through automated machine-based methodologies. Mr. Vassilev works closely with academia, industry and government agencies on the development and adoption of standards in artificial intelligence and cybersecurity and contributes to national and international standards groups. Vassilev holds a Ph.D. in mathematics from Texas A&M University. He has authored over fifty scientific papers and holds five U.S. patents. His work has been profiled in the NIST Taking Measure Blog, Fortune, Forbes, the Register, FedScoop, podcasts, webinars, and others.

John Beltz – *NIST Public Safety Communications Research*

John Beltz is the IT Security Manager for Communication Technology Laboratory (CTL), Public Safety Communications Research (PSCR) Division. He leads security-specific public safety research projects and incorporates security into all aspects of PSCR research. Additionally, he ensures that adequate security controls are in place to protect the diverse PSCR demonstration network from cybersecurity threats. Mr. Beltz's background is in network security where his prior role was managing security teams at NIST in completing A&A activities including activities such as project management, security architecture consultation, network and web application vulnerability scanning and analysis, hands-on technical testing, and reporting results to executive authorizing officials. Prior to that, he performed similar services as a senior consultant with Booz Allen Hamilton. Mr. Beltz is a proud veteran of the US Army where he served his country for 6 years. During his military career, he completed his Bachelor's Degree at Hawaii Pacific University, majoring in Computer Information Systems. He also completed a Graduate Degree at Johns Hopkins University majoring in Information and Telecommunication Systems.

Don Harriss – *NIST Public Safety Communications Research*

Donald Harriss is the Senior Network Engineer for the Communication Technology Laboratory (CTL), Public Safety Communications Research (PSCR) Division within NIST. Donald is currently researching first responder access to smart building data and associated data structures within the Public Safety Internet of Things (IoT). Mr. Harriss is the architect of the PSCR Core demonstration network and, as part of this role, performs research on core networking models and technologies used in Public Safety and enterprise networks. He received his Master's of Science in Telecommunications from the University of Colorado in Boulder and his Bachelor's of Science in Telecommunications from Murray State University in Murray, Kentucky. Mr. Harriss also has an extensive background in packet switching, routing technologies, security middleboxes, as well as the development of deployable defense systems and global satellite data networks.

Day 1 – February 7, 2024 (cont'd)

2:00 – 3:15 **Presentations – Connected Systems and Society**

Jay Stanley – *American Civil Liberties Union*

Jay Stanley is a senior policy analyst for the ACLU's Speech, Privacy, and Technology project. At the ACLU since 2001, his role is to monitor emerging technologies and help the organization think through their impact on our privacy, free speech and other civil liberties, and to help explain those implications to policymakers and the public. He has authored and co-authored numerous influential ACLU reports, policy papers, and blog posts on a wide variety of technology policy topics including aerial surveillance. Stanley's work on drones includes the 2011 ACLU report "Protecting Privacy From Aerial Surveillance," which helped bring the privacy issues surrounding domestic surveillance drones to public awareness. He has also written numerous short pieces on drone and robotics policy for the ACLU, most recently a July 2023 white paper on drones as first responder programs and authored a chapter in the book *Eyes in the Sky: Privacy and Commerce in the Age of the Drone*, (CATO Institute, 2021). He was a participant in the 2021-22 FAA BVLOS Aviation Rulemaking Committee (ARC) and in the 2023-2024 C-UAS ARC. Before joining the ACLU, he worked as an analyst at the technology research company Forrester Research and did graduate studies in 20th century American history at the University of Virginia (ABD).

Dorothy Spears-Dean – *Virginia Department of Emergency Management*

Dr. Spears-Dean joined the Virginia Department of Emergency Management (VDEM) on July 1, 2020. She leads the 9-1-1 and Geospatial Services (NGS) Bureau. This bureau is responsible for providing 9-1-1 and geospatial services to a wide range of stakeholder and constituency groups that include state and local governments. The services this bureau provides are legislatively mandated and delivered in partnership with the 9-1-1 Services and Virginia Geographic Information Services (VGIN) Advisory Boards. Prior to joining VDEM, Dr. Spears-Dean was employed by the Virginia Information Technologies Agency (VITA) as the Public Safety Communications Coordinator for the state of Virginia. She holds a Ph.D. in Public Policy from Virginia Commonwealth University, a M.B.A. from the University of Richmond, and a B.A. from The College of William and Mary. As a public safety practitioner and administrator, Dr. Spears-Dean has served in a variety of capacities. Most recently, she was an appointee to the Federal Communications Commission's Communications Security, Reliability, and Interoperability Council (CSRIC). Dr. Spears-Dean has also served as a National Association of State 9-1-1 Administrators (NASNA) Board Member and a subject matter expert for several United States Department of Homeland Security work groups. She is an accomplished author, presenter, and the recipient of the 2017 "Outstanding Government Leader" award; a national recognition presented by the NG9-1-1 Institute.

Ryan Bracken – *DroneSense*

Ryan Bracken is the Chief Product Officer & Chief Information Security Officer at DRONESENSE. DroneSense's software platform allows first responders and organizations to scale their drone programs and leverage the full capabilities of drone technology as a public safety initiative. The company's Airbase platform provides operators with the ability to attribute core data across all mission assets and pilots, automatically log flights, create customizable pilot checklists, generate custom reports and much more — expanding situational awareness in the moments when it's needed most. Prior to joining DroneSense, Ryan spent nearly twelve years as an FBI Special Agent assigned to Counterterrorism, Cyber, and Aviation operations. Ryan has FAA Commercial/Instrument and Part 107 Remote Pilot certificates and maintains a variety of SANS and (ISC)2 cyber security certifications. Ryan also worked as an Aerospace Engineer for the U.S. Air Force and holds BS and MS degrees in Aeronautical Engineering from Rensselaer Polytechnic Institute.

Michelle Hanlon – *Center for Air and Space Law, University of Mississippi*

Michelle Hanlon is the Executive Director of the Center for Air and Space Law at the University of Mississippi School of Law and a Professor of Practice within UM's Air and Space Law program. She is the Editor-in-Chief of the Journal of Space Law, the world's oldest law journal dedicated to the legal problems arising out of human activities in outer space, as well as Editor-in-Chief of the Journal of Drone Law and Policy, the first legal journal focused on law and regulations governing the operation and use of uncrewed aircraft in both civilian and military capacities. Her research and advocacy centers upon the concept of "due regard" in space law and evolving the framework necessary to assure that human exploration of space is responsible, successful and sustainable. She has done considerable work on topics related to orbital debris remediation, space solar power, small satellite constellations, environmental considerations and the protection of human heritage in space. Ms. Hanlon is also Co-Founder and President of For All Moonkind, Inc., a nonprofit corporation that is the only organization in the world focused on obtaining international legal recognition for and protection of human cultural heritage in outer space. She was instrumental in the development of the One Small Step Act in the United States, the first national legislation to acknowledge the existence of human heritage in outer space. For All Moonkind has been recognized by the United Nations as a Permanent Observer to the United Nations Committee on the Peaceful Uses of Outer Space. Most recently, Ms. Hanlon urged the United Nations to recognize and adopt temporary heritage protection zones around certain sites on the Moon as part of a legal framework for space resource utilization. Under her leadership, more than 100 space law and heritage law experts from every inhabited continent contribute to advance this important mission. Ms. Hanlon is an advisor to The Hague Institute for Global Justice Off-World Approach project. She received her B.A. in Political Science from Yale College and her J.D. magna cum laude from the Georgetown University Law Center. She earned her LLM in Air and Space Law from McGill University focusing on commercial space and the intersection of commerce and public law. She continues to provide advice and counsel in respect of all aspects of air, space and cyber law through the consulting firm of ABH Aerospace, LLC.

Day 1 – February 7, 2024 (cont'd)

2:00 – 3:15 **Presentations – Connected Systems and Society (cont'd)**

Stephen Luxion – *Alliance for System Safety of UAS through Research Excellence*

Colonel (USAF-Retired) Stephen P. Luxion is the Executive Director of ASSURE (Alliance for System Safety of UAS through Research Excellence) led by Mississippi State University. Mr. Luxion is responsible for leading the alliance of 29 of the world's leading research universities and its industry partners. ASSURE is the Federal Aviation Administration's (FAA) Center of Excellence for Unmanned Aircraft Systems (UAS). ASSURE provides the FAA a wide-ranging UAS research portfolio and conducts specific research funded by the FAA to help inform and address the key challenges to safely and efficiently integrating UAS into the National Airspace System. ASSURE also leverages its expertise, experience, and knowledge to serve others outside the FAA including current research for NASA and the Federal Emergency Management Agency (FEMA) and National Institute of Standards & Technology (NIST). Colonel Luxion is a 34-year US Air Force veteran with over 2,500 hours flying time in the F-111 Aardvark, MQ-1B Predator UAV; and the F-14A Tomcat and EA-6B Prowler while on exchange with the US Navy; including 700 hours combat time in operations over Iraq, Bosnia, and Afghanistan. For his combat efforts, Colonel Luxion was awarded the Distinguished Flying Cross for Valor, 4 Air Medals, and 7 Aerial Achievement Medals. Colonel Luxion received his Bachelor of Science degree in Computer Science and commission from the U.S. Air Force Academy in 1984. Colonel Luxion has commanded at the squadron, group and center levels and helped lead the establishment of NATO's first Aerospace Center of Excellence. Colonel Luxion is a distinguished graduate of both the USAF Fighter Weapons School and Air Command and Staff College. He is also a graduate of four Master Degree programs from Embry-Riddle, the School of Advanced Airpower Studies, and the National War College.

Day 2 – February 8, 2024

10:15 – 10:45 **Presentation – Experiences with Self-Driving Cars**

Missy Cummings – *George Mason University*

Professor Mary (Missy) Cummings received her B.S. in Mathematics from the US Naval Academy in 1988, her M.S. in Space Systems Engineering from the Naval Postgraduate School in 1994, and her Ph.D. in Systems Engineering from the University of Virginia in 2004. A naval officer and military pilot from 1988-1999, she was one of the U.S. Navy's first female fighter pilots. She is a Professor in the George Mason University College of Engineering and Computing and is the director of the Mason Autonomy and Robotics Center (MARC). She is an American Institute of Aeronautics and Astronautics (AIAA) Fellow, and recently served as the senior safety advisor to the National Highway Traffic Safety Administration. Her research interests include the application of artificial intelligence in safety-critical systems, assured autonomy**,** human-systems engineering, and the ethical and social impact of technology.

UNCREWED AIRCRAFT SYSTEMS (UAS)

February 7-8, 2024 Workshop

QR Codes for Participation

Follow-up Questions and Additional Feedback

- via Google Form
- https://bit.ly/UASQuestionsFeedback

Ongoing Workshop Dialogue

- via Slido
- https://bit.ly/UASSlido

Prioritization Exercise

- via Dotstorming
- https://bit.ly/UASVote

Workshop Reading List

- Via NIST PSCR Website
- http://bit.ly/UASReadingList

Code of Conduct for NIST Conferences

- via NIST PAO Website
- https://bit.ly/PAOCodeofConduct

UNCREWED AIRCRAFT SYSTEMS (UAS)

February 7-8, 2024 Workshop

Public Safety Scenarios

Introduction

The two breakout sessions are vital parts of this workshop, and through the procedure described in this document, we hope that we can have your participation, even if it is asynchronous.

The in-person and live online attendees will participate in two breakout sessions:

- **On the first day:** in small groups, they will consider between 3 and 5 scenarios, each with plot twists and prompting questions. They will discuss the current state of each others' response to the scenario, where the problems are, and what kinds of negative outcomes may result.

- **On the second day:** in the same groups, they will consider the same scenarios with new prompting questions. The goal is now to determine what resources, guidance, and other information would be helpful in better managing these risks, and to come up with questions that should be asked in the immediate term.

For attendees participating asynchronously: We invite you to perform both parts at the same time. If you are able to provide your input by noon on the 8th of February US Eastern time (UTC-5), we can combine your input with those who are participating in-person and live. Of course, we also welcome your input at any time afterwards as well. Please see the next page for additional instruction.

Scenario Prompts

Day 1

1. What is the most likely or plausible worst-case result or outcome?
2. What are the potential tools ***currently*** available (technology, procedures, alternative method, etc.)?
3. What are the ***current*** operational constraints (gaps in tools, technology, procedures, safety, timing, risks, etc.)?

Note for each question:

- Consider **impacts broadly**, including to the **mission, public safety personnel, the public, property, perception of the organization, and so-on**.
- Consider **current best, average, and minimum** practice.

Day 2

1. What technical and procedural measures could manage this risk?
2. What residual risks are unavoidable?
3. How do these inform the cost/benefit analysis?

Instructions For Asynchronous Participation:

1. If you have time, we recommend that you have watched the talks up until this point.
2. Read the scenario from the top.
3. As you work through each paragraph, think about the questions in the previous section (**Scenario Prompts**). Don't feel obliged to write these down unless you would like! Note that not all of them may be relevant to the scenario, or to your sector or area of expertise.
4. Continue reading the scenario and repeat (2). Subsequent paragraphs may change your answers!
5. When you get to the end of the scenario, if you would like to, we would welcome you to write down and send us:
    - Your top 1-3 obvious questions that would help a fire chief, police chief, or other public safety management person, to understand their possible risks.
    - Your top 1-3 non-obvious questions as above.
    - Any particularly profound or important thoughts you have about any of the prompting questions or scenarios.

Workshop Scenarios:

Scenario 1: Changing Maps

The 911 call center receives two calls about a person acting strangely and appearing to be holding a weapon in the vicinity of new buildings in an industrial park. The dispatcher decides to send a drone to the scene using the Drone as First Responder (DFR) system which shows the dispatcher the most direct path to the building. It proposes that the best view to see the person at the scene is from the park across the street. The drone is launched, climbs to 300 feet, flies to the scene, then descends to 100 feet. The dispatcher monitors the expected path of the drone from their remote console and discovers the park is now a construction site that does not yet appear in the DFR system's map. Unfortunately, they only realize this as the drone is descending. Due to delays in the system, the dispatcher cannot intervene in time. The AI on the UAS must figure out what to do to avoid unexpected obstacles in the path.

Scenario 2: HAZMAT Accident

The dispatch center receives a call that a tanker truck crash occurred on the interstate that runs through the jurisdiction. A HAZMAT fire team is dispatched as well as a drone from the Drone as First Responder (DFR) system. The drone is the first to arrive to the scene. The remote UAS pilot of the DFR performs a quick analysis of the situation and observes smoke coming from the nearby burning vehicles. The pilot switches over to the Infrared Camera (IR), however, objects are still difficult to decipher. The DFR's computer vision falsely identifies multiple people on the ground and it's not clear where the fire source is because the identifying boxes frequently change the objects of focus. The pilot has had experience with misclassification of objects before that provided false positives, so she knew there were likely no people in the vicinity. A gust of wind provides temporary visibility of the area around the crashed truck and reveals no visible fire; however, a heat signature is still being observed in the IR footage. From this information, both the HAZMAT specialist and UAS pilot determine that the truck is carrying ethanol and flames that are nearly invisible to the human eye. Firefighters arriving at the scene are able to use this information to safely extinguish the fire and evacuate the area.

Workshop (Cont'd)

Scenario 3: Wildfire

The American West has been experiencing an especially dry season resulting in multiple wildfires. One fire has been burning for multiple days, burned over 50,000 acres, and now threatening multiple towns. The region's wildland firefighting group uses a Drone as First Responder (DFR) system integrated with ATAK (Android Team Awareness Kit) and other systems. The group decides to create a back-burn fire by using their UAS "Dragonball" system, which creates controlled fires in advance of the larger wildfire. The idea is to create a controlled burn to clear an area of combustible material and help stop the spread of the larger fire.

The area of interest for deploying the dragon balls is situated on the west side of a mountain canyon. The east side of the canyon has a large antenna array atop the mountain that serves a town further east. There are no established fire roads to access the canyon on the east side, however, a remote pilot is deployed to the antenna array to observe the mission and take manual control, if necessary. The DFR deploys the drone autonomously using a preplanned flight path. As the UAS flies closer, the DFR pilot notices the drone is off course by almost half a mile, putting it on the wrong side of the canyon. The remote pilot also notices this and immediately activates manual control of the UAS, however, the controller does not connect due to interference. After multiple attempts, the team is unable to abort the mission and the drone drops the propellant in the wrong spot.

Scenario 4: Public Event

The state fair is held at Techtown every year and they expect this year's event will be its biggest ever. Such events are a perfect use for the town's Drone as First Responder (DFR) system for surveillance and response. However, previous experience has found that civilian use of drones also causes disruptions in their operations. To help counteract this, Techtown's DFR system is equipped to track remote-IDs to help responders locate drones as well as pilots.

On the first night, the UAS is deployed to monitor the area around the venue. After a few minutes, a different drone shows up on the tracking system with a remote-ID identical to the remote-ID of the DFR UAS. Likewise, the GPS data received by the remote-ID of the other drone is identical as well. The DFR system doesn't know how to distinguish between the two drones which prompts an error on the operator screen. The system interprets the duplication as a malfunction, which automatically initiates a landing sequence. The drone completes its landing, but once on the ground, the drone's video feed is immediately cut off and command & control are lost. Concert security is dispatched to retrieve the aircraft in a nearby field, however the drone can not be located.

Workshop Scenarios (Cont'd)

Scenario 5: Eavesdropping

Techtown's drone program has come under public scrutiny since the implementation of the Drone as First Responder (DFR) system. Many citizens have become concerned that the system is used to unnecessarily surveil citizens and profile certain demographic groups. Some privacy groups have also called for greater program transparency and the release of UAS video, telemetry, as well as datasets used to train the DFR's AI functions. Due to the confidential and proprietary nature of the data, and pending legal cases, it has become difficult for Techtown to meet these requests.

One day while browsing a popular social media platform, Anytown's police chief saw a post of sensitive drone footage from a police event that occurred earlier in the week. The post included video data that would only have been observed by the DFR pilot which included AI-generated overlays and text. As an aside, the AI in this instance presented false information about the suspect which led to a false arrest.

An investigation was launched about the data leak and, with the assistance of the social media company, information about the original social media post helped apprehend the suspect. The suspect revealed that they were able to obtain the information by using a wireless ethernet sniffer application while standing near the "drone-in-a-box" launch point which was located atop a building. The wireless network in question was designed to be used as a maintenance access point to perform configuration updates without having to connect directly to the drone box. It turns out that the maintenance access point did not have a secure configuration and still had its factory default settings. To complicate matters more, the access point was not designed to interface with drone video and telemetry data and should've been firewalled from other DFR systems.

Extra Scenarios

Scenario 6: Loss of Connectivity 1

One day, during the morning rush hour, dispatch receives a call reporting a multiple-vehicle crash. The location of the incident occurred on a multi-lane highway. The dispatch deploys a drone using the Drone as First Responder (DFR) system in addition to police and fire units. The DFR drone arrived at the crash scene first and revealed that a semi-truck carrying potentially toxic liquids was involved in the crash.

A first responder with HAZMAT training is tasked with examining the DFR system's live video feed. This was the first time the HAZMAT specialist logged into the DFR system and had not been previously enrolled in the system. IT support staff is available to enroll the specialist with little delay. While performing the enrollment, all the DFR users and first responders suddenly lose remote control capability of the UAS as well as video feed.

Scenario 7: Loss of Connectivity 2

Techtown uses a Drone as First Responder (DFR) system with an AI-deterministic abort protocol to make navigation decisions autonomously. One day, while on a mission, the remote pilot loses connectivity due to a configuration error made by IT staff. The abort protocol is designed for the drone to initiate a preplanned procedure if the remote pilot loses connection to the drone after 15 seconds of communications loss. At this point, the drone will “backtrack” its initial flight plan until it reaches 300 feet Above Ground Level (AGL) so it doesn’t interfere with operations on the ground. Next, the drone waits to reconnect and the amount of time it waits is a function of having 25% remaining battery capacity to make the return trip or return-to-home (RTH) and land. The drone also considers environmental conditions based on previous flights.

Scenario 8: Strange Behavior

About an hour before sunset, Techtown Fire and Rescue is called to respond to a fire at the electrical substation that feeds one of the industrial parks. The first responders on the scene deploy a UAS to get a better look at the situation.

The UAS flies close to the substation but then, about 100 feet away, it begins behaving erratically, refusing to go closer, and responding sluggishly to the controls. The substation is not coming up as a no-fly area and no warnings are being displayed in the operator interface.

Extra Scenarios (Cont'd)

Scenario 9: EMS Scenario

Techtown Community Hospital utilizes the city's Drone as First Responder (DFR) system for some of its ambulatory and emergency medical services. Techtown is surrounded by mountainous terrain that is difficult to reach by vehicle or foot. The DFR system allows EMS responders to quickly transport vital medical services and supplies to hard-to-reach areas that may otherwise take several hours to reach.

One day, a call comes in about a person experiencing a heart attack near the Banana trailhead. The drive to the trailhead is nearly an hour away traversing rough off-road vehicle trails; however, it's only an 8-minute flight from the nearest UAV launch pad. Dispatch immediately deploys a drone with an integrated defibrillator with voice-command system to the Banana trailhead. Due to intermittent cellular service, EMS dispatch doesn't get an update with the drone's flight status until it's further up the mountain. When the update occurs, dispatch discovers that the drone is heading in the wrong direction. It turns out that instead of Banana, the system mistook the verbal command as Bandana, which happens to be the name of a trail on a nearby mountain.

Scenario 10: Chain of Custody and Evidence Manipulation

Techtown uses a Drone as First Responder (DFR) system that integrates with cloud features that enhance AI functionality as well as streamline chain-of-custody processes and logging. AI functionality collates events to all data including video, telemetry data, pilot information, black-box data, AI-generated prompts, and more. This system also integrates into the town's other digital evidence systems to associate assets, such as body cameras, records, and CCTV files.

One day, an evidence technician is reviewing an old report on a high-profile case that resulted in imprisonment for the suspect. While analyzing the output, the technician discovered that some of the metadata on the report contained timestamp discrepancies. Due to the volume of data for the case, this was not captured by people analyzing the data, nor was it flagged by the collection system. The timestamp data on the actual video differed from the encoded metadata. When the AI initially collated the data, it used the metadata timestamp instead of the timestamp embedded in the video. The video in question did not contain a clear view of the suspect, however, it was assumed based on this piece of evidence and the suspect was considered guilty. If the timestamp on the video is correct, then the finding would dispute the suspect's actions. Additionally, it would potentially uncover evidence manipulation and question the integrity of the AI functionality.

Extra Scenarios (Cont'd)

Scenario 11: Supply Chain Attack

Techtown has a large fleet of UAS assets that are mostly integrated into Techtown's Drone as First Responder (DFR) system. Techtown is going through the process of removing older UAS assets that are either not compatible with the DFR system or can no longer be used due to federally imposed bans on certain foreign-made drones. To help save on costs, Techtown decides to purchase optical packages for the drones from a lower-cost reseller. The optics integrate into the DFR's computer vision systems to perform onboard processing, which helps reduce latency induced by cloud-based processing handoffs.

When Techtown started using the new optics, many operators were reporting an increase in misidentifications by the AI functions. A self-diagnostic and comparison of the data with the cloud-based system revealed no issues. These misidentifications were only noticed by the human operators, but the software diagnosis reported no issues. Coincidentally, the agency's network operations department reported a large amount of outbound data, sourced from the DFR system, destined for an IP address located in a foreign adversarial country. One of the team's UAS repair technicians decides to disassemble one of the new optics packages and discovered components sourced from the same foreign adversarial country. Further inspection and comparison to a demo provided by a different optics reseller reveals that the components Techtown bought were counterfeit and compromised with malicious components.

Scenario 12: Chain of Custody

Techtown Police are responding to reports of a robbery with a firearm near a residential area. A Drone as First Responder (DFR) UAS is dispatched, zooms in, locates someone matching the description who is holding what looks to be a handgun. The operator zooms in further and is able to get a good picture of their face.

The UAS then loses sight of the person but someone matching the picture taken from the UAS is later found by officers and taken in for questioning. No weapon was found on the person or in a search of the nearby area.

In court, the saved pictures from the UAS are used as evidence to link the person to the robbery with a firearm. The defense challenges the chain of custody of the evidence from the UAS and, using their cellphone camera as an example, proposes that the image could have been altered by someone or by some AI enhancement.

Extra Scenarios (Cont'd)

Scenario 13: Update Issues

After software updates, Techtown Fire and Rescue pilots fly regular test missions in the local stadium where the Standard Test Methods for Small Uncrewed Aircraft Systems are embedded. This ensures that as much as is practical, each test mission is similar.

During the latest post-update test mission, the UAS is seen to behave erratically during a couple of the embedded tests. Performing repeated tests over successive days with different (recently updated) copies of the same UAS revealed similar behavior.

Example “Top 10” Questions

- "What documentation and support do you offer to allow us to determine the residual Cybersecurity and AI Risk associated with using your system, such as example policy guides?"
- "What aspects of the system's behavior depends on AI? How does the behavior of the AI system affect safety? What guarantees can be made about the limits of the AI system?"
- "Will my data be used to help improve the system or be used in training data? Will this data be anonymized, and are there opt-in, opt-out procedures in place?"
- "What is your policy with regard to reporting cyber attacks to us? What steps do you have to maintain continuity of service in the event of a cyber attack? Can you show us your disaster and recovery plan?"
- "How is the performance and security of updates to the software, and any AI models on the system, verified? If any changes in behavior affect risk, how is this communicated?"
- "When the system makes a decision that we don't agree with, what options do we have for performing root cause analysis to determine how the decision was made and where a similar decision might be made?"

UNCREWED AIRCRAFT SYSTEMS (UAS)

February 7-8, 2024 Workshop

Glossary of Terms*

Artificial Intelligence (AI): Engineered systems that generate outputs such as content, forecasts, recommendations or decisions for a given set of human-defined objectives.

Computer Aided Dispatch (CAD): Systems utilized by dispatchers to record calls, identify the status and location of responders in the field, and effectively dispatch responder personnel. Emergency responders in the field can receive messages initiated by CAD systems. CAD systems may also interface with GIS and other systems. A unified CAD (UCAD) system interfaces with multiple agencies and provides communication across multiple agencies and jurisdictions.

Cybersecurity: The process of protecting information by preventing, detecting, and responding to attacks.

Drone as First Responder (DFR): A program whereby uncrewed aircraft systems (UAS), or drones, are pre-positioned in a service area (such as the area served by a police department), ready to be launched immediately in response to an emergency call for service.

Federal Aviation Administration (FAA): An agency of the U.S. Department of Transportation that regulates civil aviation.

Geographic Information System (GIS): A computer system that analyzes and displays geographically referenced information. It uses data that is attached to a unique location.

National Institute of Standards and Technology (NIST): An agency of the U.S. Department of Commerce with the mission of promoting U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

Public Safety: Those who protect lives and property during day-to-day operations, large scale events, and emergencies (e.g., Fire, Police, Search and Rescue, Hazmat, Contractors, Industry and Resources, Utilities, and Forest/Land Management).

**Note: these definitions are for the purposes of scoping this workshop.*

Glossary of Terms* (Cont'd)

Public Safety Communications Research Division (PSCR): The primary federal laboratory conducting research, development, testing, and evaluation for public safety communications technologies.

Risk: Engineered systems that generate outputs such as content, forecasts, A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.

Risk Management: The process of identifying, assessing, and responding to risk.

Uncrewed Aircraft System (UAS): An uncrewed aircraft and the equipment necessary for the safe and efficient operation of that aircraft.

**Note: these definitions are for the purposes of scoping this workshop.*

UNCREWED AIRCRAFT SYSTEMS (UAS)

February 7-8, 2024 Workshop

PSCR UAS Portfolio Team

We greatly appreciate you taking the time to support these efforts and hope to stay in touch:

Raymond Sheh *UAS Research Lead* raymond.sheh@nist.gov	**Terese Manley** *UAS Portfolio Lead* terese.manley@nist.gov	**Ellen Ryan** *Deputy Division Chief* ellen.ryan@nist.gov
Don Harriss *UAS Technical Lead* donald.harriss@nist.gov	**General Inquiries** *PSCR UAS Portfolio Team* psprizes@nist.gov	**Stephanie Layman** *UAS Portfolio Support* stephanie.layman@nist.gov

And consider joining our ongoing Working Group: